What is Claimed Is:

1. A method for encrypting data, comprising the steps of:

reading a plaintext data block from a memory;

storing the plaintext data block in an input buffer;

encrypting the plaintext data block in the input buffer using a first mode to generate a first ciphertext;

storing the first ciphertext in an output buffer; and

encrypting the plaintext data block in the input buffer using a second mode to generate a second ciphertext.

2. The method of claim 1, wherein encryption is performed using CCM.

3. The method of claim 1, wherein the first mode comprises a CTR (counter) mode.

4. The method of claim 1, wherein the second mode comprises a CBC (cipher block chaining) mode.

5. The method of claim 1, further comprising the step of storing the second ciphertext in an initialization vector buffer.

6. The method of claim 1, further comprising the step of storing the second ciphertext in the output buffer.

7. A method for encrypting data in a block encryption module of a cryptographic system, comprising the steps of:

reading a plaintext data block from a memory external to the block encryption module;

storing the plaintext data block in an input buffer of the block encryption module;

encrypting the plaintext data block in the input buffer using a first mode to generate a first ciphertext;

storing the first ciphertext in an output buffer of the block encryption module; and

encrypting the plaintext data block in the input buffer using a second mode to generate a second ciphertext.

8. The method of claim 7, wherein encryption is performed using CCM, wherein the first mode comprises a CTR (counter) mode and wherein the second mode comprises a CBC (cipher block chaining) mode.

9. The method of claim 8, further comprising the step of storing the second ciphertext in an IV (initialization vector) buffer.

10. The method of claim 8, further comprising the step of storing the second ciphertext in the output buffer.

11. A method for decrypting data, comprising the steps of:

reading a ciphertext data block from a memory;

storing the ciphertext data block in an input buffer;

decrypting the ciphertext data block in the input buffer using a first mode to generate a plaintext;

storing the plaintext in the input buffer, an output buffer or both; and

encrypting the plaintext in the input buffer or the output buffer using a second mode to generate a ciphertext.

12. The method of claim 11, further comprising converting one or more bits of the plaintext to logic level "0" before encrypting the plaintext using the second mode.

13. A cryptographic system, comprising:

means for reading a plaintext data block from a memory;

means for storing the plaintext data block in an input buffer;

means for encrypting the plaintext data block in the input buffer using a first mode to generate a first ciphertext;

means for storing the first ciphertext in an output buffer; and

means for encrypting the plaintext data block in the input buffer using a second mode to generate a second ciphertext.

14. The cryptographic system of claim 13, further comprising:

means for reading a ciphertext data block from the memory;

means for storing the ciphertext data block in the input buffer;

means for decrypting the ciphertext data block in the input buffer using a first mode to generate a plaintext;

means for storing the plaintext in the input buffer, an output buffer or both; and

means for encrypting the plaintext in the input buffer or the output buffer using a second mode to generate a ciphertext.

15. A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform method steps for encrypting data, the method steps comprising:

reading a plaintext data block from a memory;

storing the plaintext data block in an input buffer;

encrypting the plaintext data block in the input buffer using a first mode to generate a first ciphertext;

storing the first ciphertext in an output buffer; and

encrypting the plaintext data block in the input buffer using a second mode to generate a second ciphertext.

16. A cryptographic apparatus, comprising:

a memory controller that reads a block of data from a memory;

an input buffer that stores a block of data read from the memory;

an encryption module that encrypts the block of data stored in the input buffer using one of a plurality of modes of operation supported by the encryption module

including a CTR (counter) mode, CBC (cipher block chaining) mode and CCM (CTR and CBC-MAC (message authentication code) mode;

an output buffer that stores the data encrypted by the encryption module; and

a control unit that generates control signals to control the memory controller, the input and output buffers and the block encryption module, wherein the control signals comprise a mode control signal that specifies a mode of operation of the encryption module.

17. The cryptographic apparatus of claim 16, wherein the encryption module comprises:

a PL (preload) register that stores data associated with a CTR mode;

an adder module that adds a logic "1" to data output from the PL register;

an IV (initialization vector) register that stores data associated with a CBC mode;

a data input register that stores an data block input from the input buffer;

a data output register that stores a data block to be output to the data output buffer;

a first logic operator that performs an exclusive-or (XOR) operation on data in the IV register and the data input register;

a block cipher module; and

a second logic operator that performs an XOR operation on data output from the block cipher module and data in the input register.

18. The cryptographic system of claim 17, further comprising a plurality of switching devices that respond to a mode control signal by selectively routing data paths of the encryption module to execute a mode of operation specified by the mode control signal.

19. The cryptographic apparatus of claim 18, wherein the switching devices comprise a first multiplexer that selectively routes an output of the PL register or an output of the first logic operator to an input of the block cipher module in response to a mode control signal.

20. The cryptographic apparatus of claim 18, wherein the switching devices comprise a second multiplexer that selectively routes an output of the block cipher module to an input of the IV register or to an input of the second logic operator.

21. The cryptographic apparatus of claim 18, wherein the switching devices comprise a third multiplexer that selectively routes an output of the data input register to either an input of the first logic operator or to an input to the second logic operator, depending on a mode of operation specified by a mode control signal.

22. The cryptographic apparatus of claim 18, wherein the switching devices comprise a third multiplexer that selectively routes an output of the data input register or data output register to an input of the first logic operator or the second logic operator, depending on a mode of operation specified by a mode control signal.

23. The cryptographic apparatus of claim 17, further comprising a mute module for "0" padding a block of plaintext in the data input register to be input to the first logic operator.

24. The cryptographic apparatus of claim 17, wherein in a CCM mode of operation, a block of plaintext stored in the data input buffer is applied to a CTR mode and a CBC-MAC mode of operation for the CCM mode.

25. The cryptographic apparatus of claim 17, wherein in a CCM mode of operation, a block of plaintext, which is generated by applying a CTR mode of operation on a block of ciphertext stored in the data input register, is applied to a CBC-MAC mode of operation for the CCM mode.

26. A communications system comprising the cryptographic apparatus of claim 16.